Management System: Information Resource Management (IRM)

Subject Area: Applications and Software Development

Management System Owner: Ward Best
Point of Contact: Lisa Rawls

Issue Date: 9/4/2012
CBC MS Revision: 0

1.0 Introduction

This subject area describes the process for designing, developing and supporting web-based applications when commercial products are not adequate to meet user requirements or when developing an in-house product is a cost effective option; and ensures the appropriate level of software quality assurance is applied to software applications whether or not they are developed or supported by the Office of Information Management (IRM).

2.0 Contents

The table below represents procedures and procedure content specific to this Subject Area.

Procedures	Procedure Content
1. Procedure 1 – Applications and Software Development	• Describes the duties of the Content Owner or Manager in the development process of applications and software

3.0 Exhibits/Forms

- Checklists for Software Classification Determination
- Software Evaluation
- Records Management Compliance Checklist
- Software Change Request

4.0 Related Information

- Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) – Application Security Checklist (http://iase.disa.mil/stigs/index.html)
- FIPS 127-2 – Standards for Database Language SQL (http://csrc.nist.gov/publications/PubsFIPS.html)
- IMP-8308-02 – Configuration Management of Computer Systems and Networks
- DOE O 414.D – Quality Assurance (https://www.directives.doe.gov/directives/current-directives/directives-current-400-series)
- PS-563-01 – Cyber Security Master Policy, Attachment 10.14, Identification and Authentication (IA) Policy
- DoD 5015.2-STD – Electronic Records Management Software Application Criteria Standard, 2007 (http://www.dtic.mil/whs/directives/corres/pdf/501502std.pdf)
- Records Policy, Guide to IT Capital Planning and Investment Control (CPIC), September 2005 (http://www.hhs.gov/ocio/policy/2005-0005.001.html)

5.0 Requirements

Document	**Title**
IMP-8308-03 (under development)	Software Application Development and Management
PL-240-08	Cyber Security – System Security Plan for General Support System – OUO
PS-240-06	Control of Unclassified Electronic Information

6.0 Definitions

Term	**Definition**
Alpha Testing	Testing of applications with inert (made up) data.
Authorizer	A person given authority or official power to place a written signature on a message or a document, or the approval of data.
Beta Testing	Testing of applications with “real” data.

Term	**Definition**
Content Manager	Individual assigned by the Content Owner to manage the development of the application and to ensure the integrity of the data.
Content Owner	The EMCBC Assistant Director responsible for the content and functionality within the given application or system.
Developer	IRM staff responsible for coding, testing and placing the application into production.
Digital Authorization	Any electronic approval of information or data. Digital authorization requires that the identity of the authorizer is authenticated. It also requires security measures to ensure that the message is unchanged after the authorization.
Digital Authorization Database	A central relational database containing Authorizing data that can be access by any authorized relational database and/or application developed and/or maintained by the EMCBC regardless of format.
Hash	A hash algorithm computes a condensed representation of electronic data (message). When a message is input to a hash algorithm, the result is an output called a message digest. Hash algorithms are called secure when, for a given algorithm, it is computationally infeasible 1) to find a message that corresponds to a given message digest, or 2) to find two different messages that produce the same message digest. FIPS 180-2
Requesting Application	Any relational database and/or application developed and/or maintained by the EMCBC that has been authorized by the Content Owner or System Owner to access the Digital Authorization Database.
System Owner	The lead individual that has overall responsibility for the implementation for any given application, usually the Assistant Director for IRM.